# Department of Homeland Security
# Information Analysis and Infrastructure Protection
# Daily Open Source Infrastructure Report for 12 September 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

## Daily Overview

- KSDK−TV reports Fire Department officials are classifying the gas leak in downtown St. Louis, on September 11, as major and say some unknown perpetrator caused it. (See item 3)
- The New York Times reports the United States has barred five pilots from the Saudi national airline from flying to the United States after their names turned up this summer on watch lists of people tied to international terrorism. (See item 8)
- Agriculture Online reports a California economic development corporation is pointing out a terrorist risk to rail service in this country that shows potential to cause significant harm to the economy. (See item 9)
- U.S. Department of State: Public Announcement concerning Worldwide Caution (See item 29)



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *September 11, Reuters* — **Fire at Susquehanna nuclear plant.** PPL Corp.'s 1,000 megawatt Susquehanna 1 nuclear unit in Pennsylvania was running at 70 percent power on Thursday, September 11, down from full power on Wednesday, September 10, the U.S. Nuclear

Regulatory Commission said in its power reactor status report. **The unit, located in Luzerne County, PA, reduced output after the plant's fire brigade quickly extinguished a small oil fire late Wednesday night,** PPL said in a separate statement. The fire started at 11:14 p.m. EDT on one of three pumps that provide water to the Unit 1 reactor. The water is boiled to make steam, which drives the turbine to generate electricity. The fire was on a pump not directly related to the plant's nuclear safety systems, which were not affected by the incident. There were no injuries or any threat to the general public as a result of this incident, Joe Scopelliti, spokesperson for the plant, said in the statement. Scopelliti said the company was investigating the cause of the fire, which was put out in eight minutes.
Source: http://biz.yahoo.com/rc/030911/utilities_ppl_susquehanna_1.h tml

2. *September 11, Associated Press* — **Electrical grid vulnerable to hackers.** Since last month's Northeast Blackout, utilities have accelerated plans to automate the electric grid, replacing aging monitoring systems with digital switches and other high−tech gear. But those very improvements are making the electricity supply vulnerable to a different kind of peril: computer viruses and hackers who could black out substations, cities or entire states. **Researchers working for the U.S., Canadian and British governments have already sniffed out "back doors" in the digital relays and control room technology that increasingly direct electricity flow in North America.** With a few focused keystrokes, they say, they could shut the computer gear down − or change settings in ways that might trigger cascading blackouts. "I know enough about where the holes are," said Eric Byres, a cybersecurity researcher for critical infrastructure at the British Columbia Institute of Technology in Vancouver, Canada. "My team and I could shut down the grid. Not the whole North American grid, but a state, sure." Security experts have warned about the grid's growing vulnerabilities before, especially after U.S. National Security Agency hackers showed they could break into grid control networks in 1998. With an expected spate of post−blackout upgrades, the computer−heavy grid will be even more vulnerable to terrorists and hackers, they say.
Source: http://seattlepi.nwsource.com/business/aptech_story.asp?cate gory=1700&slug=Blackout%20Hacking

3. *September 11, KSDK−TV (St. Louis, MO)* — **Major gas leak in downtown St. Louis forces evacuations. Fire Department officials are classifying the gas leak in downtown St. Louis, MO, on Thursday, September 11, as major and say some unknown perpetrator caused it. Officials are looking at construction equipment on Olive between 10th and 11th streets that may have caused the leak.** The leak was shut−off by way of a gas main valve. Laclede Gas repair crews are working to find the source of the leak which they believe is located under the street. A spokesperson for the St. Louis Fire Department says **despite the shutdown via the valve, there is still a very heavy concentration of gas odor at the scene. The gas is apparently contained in several buildings and the adjoining sewer lines are being used as a way to ventilate the gas out.** The sewer lids have been removed and the windows of the buildings opened to air things out.
Source: http://www.ksdk.com/news/news_article_lc.asp?storyid=46706

[Return to top]

## Chemical Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

4. *September 03, The Office of Naval Research* — **Breaking communications stovepipes with an all−digital receiver. The Office of Naval Research (ONR) has moved the Navy−and all the services−a big step closer to needing only one radio to talk to the many already in service with the development of an all−digital radio receiver. The inherent accuracy and very high processing speed enable these receivers to handle multiple simultaneous signals spread over considerably wider communications bandwidths.** A small New York State company is building the new digital receivers. Deborah Van Vechten, program officer in ONR's Electronics division, says that this company will deliver a demonstration receiver that simultaneously digitizes all the signals in the most critical over−the−horizon military communications bands (HF and VHF) and uses a technique called software−controlled digital filtering to select the signals to output. **Such software control is the fundamental innovation required to realize the Department of Defense's vision for the joint tactical radio system (JTRS) program, now underway, which seeks to develop a generic radio for all the services.** This program addresses the lack of interoperability among the stovepipe−type tactical radios, in use aboard ships, aircraft, and carried by ground units.
   Source: http://www.onr.navy.mil/media/tipoff_display.asp?ID=46#1

[Return to top]

## Banking and Finance Sector

5. *September 11, Star−Telegram (Fort Worth, TX)* — **Police bust identity−theft ring.** Sixteen people have been arrested in connection with a forgery ring, concentrating most of their crimes in Tarrant County, TX. The suspects had specialized roles in the operation, such as stealing mail or passing counterfeit checks, investigators said. "They would interchange information, they would share identities, they would teach each other scams," Arlington, TX, police Detective Kyle Dishko said. Most of the members of the eight−man, eight−woman group have been arrested on forgery, identity theft and drug charges. **Through arrests and interviews, police learned that the suspects, who met regularly, each had one thing they would do better than the others, Arlington Detective Kyle Gibson said. Those with computer and desktop publishing skills would create counterfeit checks and fake IDs while others were responsible for stealing the mail or passing the forged checks.** Since August 2002, police and U.S. postal inspectors have seized hundreds of pieces of stolen mail, forged checks, fake identities and computer files that list personal information for at least 402 people, the majority of them from Arlington, said Detective Randy Holton. **The suspects had collected the identities through mailbox theft, vehicle burglaries and public−record websites.**
   Source: http://www.dfw.com/mld/dfw/news/6744725.htm

[Return to top]

## Transportation Sector

6. *September 11, Associated Press* — **Gaps remain in post−9/11 transportation security.** When a man recently stowed away in a cargo plane from New York to Dallas, TX, by shipping himself in a wooden crate, it raised questions about transportation security nearly two years after terrorists turned jetliners into missiles. **"Transportation security is at its highest level ever, particularly aviation security," said Sen. John McCain, R−AZ, chairman of the Senate Commerce Committee, said Tuesday. "However, we need to remain vigilant across all modes of transportation."** Two months after the 2001 attacks, Congress created the Transportation Security Administration to protect aviation, shipping and transit. Still, Peter Guerrero, director of physical infrastructure questions for the General Accounting Office, said much more needs to be done. **Guerrero, whose agency is the investigative arm for Congress, testified before McCain's committee that it could cost hundreds of billions of dollars to secure the country's transportation network −− 3.9 million miles of roads, 600,000 bridges, 361 ports and more than 5,000 public−use airports.** For example, Guerrero, in written testimony, pointed out that only a small amount of 12.5 million tons of cargo is inspected before it is shipped by air every year. Another major worry is that terrorists could use shoulder−fired missiles to bring down an airliner.
Source: http://www.cnn.com/2003/TRAVEL/09/10/transportation.security .ap/index.html

7. *September 11, New York Times* — **Slip−on shoes, long waits: air travelers still adjusting. Airports, where the attacks of September 11, 2001, were launched, are where the most Americans, about a billion passengers last year, have seen the post−September 11 changes up close.** Some of those changes are big and obvious: the 49,600 federal security agents in crisp white shirts, mammoth bag−screening machines, hundreds of pilots carrying guns. Logan Airport here, where the two planes that hit the World Trade Center took off, has added 61 state troopers since the attacks. Across the country, there are fewer flights, especially direct ones, and fewer passengers. **Two years after the attacks, frequent fliers seem to have settled in to their new world of travel. But a tour of airports large and small shows people making subtle adjustments, ones that suggest both a sense of resolve and a continued sense of vulnerability. Travelers have bought post−9/11 shoes (slip−ons, no metal) and bags (bigger, more compartments) to smooth the ride through security. People have stopped wearing knee braces and removed medical devices rather than deal with a strip search at security.** By all accounts, the biggest adjustment has been arriving for flights earlier, up to two hours instead of 15 minutes.
Source: http://www.nytimes.com/2003/09/11/national/11AIRL.html?pagew anted=1

8. *September 11, New York Times* — **U.S. bars five Saudi pilots from U.S.** The United States has barred five pilots from the Saudi national airline from flying to the United States after their names turned up this summer on watch lists of people tied to international terrorism, Bush administration officials said today. **Saudi Arabian Airlines and the five pilots, all Saudi citizens, were notified several days ago that the pilots would no longer be allowed to enter the United States under any circumstances,** the officials said. The airline has regular flights to New York and Washington. The move to bar the Saudi pilots came as a result of an expanded effort this summer by the Department of Homeland Security to scrutinize the backgrounds of pilots flying for foreign airlines to the United States. Department officials said they stepped up the effort as a result of intelligence reports suggesting that al Qaeda planned to hijack or attack commercial planes entering the United States. American officials would not

describe the evidence that showed that the five might have ties to al Qaeda and other terrorist groups, **but they said the names had turned up on one of two watch lists: one compiled by a federal border intelligence center in El Paso, the other compiled by a national terrorism task force that includes the FBI.**
Source: http://www.nytimes.com/2003/09/11/national/11PILO.html

9. *September 11, Agriculture Online* — **Potential terrorist threat to U.S. railways.** As the U.S. commemorates the second anniversary of the terrorist attacks of September 11, 2001, a California group is pointing out a terrorist risk to rail service in this country that shows potential to cause significant harm to the economy. **"The threat of terrorism is real on strategic rail corridors with passenger and freight rail service and we believe that al Qaeda's apparent interest in rail attacks should be a call to action,"** says Elsa Lee, a counter terrorism expert. Such an attack could cost the U.S. economy more than $400 million each day of a resulting shut down, according to the study, published by Los Angeles Economic Development Corporation (LAEDC) in conjunction with the Orange North−American Trade Rail Access Corridor (OnTrac) Joint Powers Authority **Terrorist attacks on rail transportation are not unprecedented, the authors say. Most appear to have been aimed at passenger, rather than freight rail. "Although the freight rail network has not yet been exploited by any substantial acts of terrorism, recent FBI warnings about al Qaeda's apparent interest in rail attacks should be cause for concern," they say.** History has shown that terrorist methods used in other countries, including suicide bombings and train attacks, eventually surface in the U.S., the authors say, noting **"In 2003, nine derailment devices were reported stolen in the Midwest."**
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDetail__ANewsindex_html___50589___1

10. *September 11, Government Computer News* — **FAA begins building oceanic air traffic system.** The Federal Aviation Administration (FAA) has accepted the initial hardware and software for a new air traffic management system that will improve separation of aircraft flying over U.S. oceanic airspace, FAA said yesterday. **Software called Advanced Technologies and Oceanic Procedures (ATOP) will replace FAA's existing systems and procedures. ATOP will let controllers reduce the space between airborne aircraft while preserving passenger safety and, in the process, improve fuel efficiency and costs.** The system, which FAA accepted July 31, will integrate flight data processing, detect conflicts between aircraft and provide data link and surveillance capabilities. FAA expects to begin using the system next June, said Charlie Keegan, FAA's associate administrator for research and acquisitions. Full system operation is slated for 2005. By that time, the highest percentage increase in air traffic is projected to occur across the Atlantic and Pacific oceans, FAA said.
Source: http://www.gcn.com/vol1_no1/daily−updates/23478−1.html

11. *September 11, CBC (New Brunswick)* — **Canada's new gamma ray imaging system.** The Port of Saint John (Canada) has unveiled a $2 million high−tech imaging system that customs officials say will improve their ability to check containers and trucks coming into the country. **The machine is called a mobile VACIS, or vehicle and cargo inspection system. It uses gamma rays to see right through shipping containers like an X−ray. It speeds up the inspection of cargo crossing the border.** Federal Revenue Minister Elinor Caplan says it's just one element of increased border security since the terrorist attacks on New York City and

Washington two years ago. **The port has improved its security since the attacks on September 11, 2001. What was once a completely open facility is now enclosed by fencing, and regular port users can't get in without photo identification. Small compartments in containers often go undetected, and Port Superintendent Gary Stewart says the gamma ray machine can detect the smallest of aberrations in a large container.** Eleven of the units will be up and running at border points across the country by the end of the year. Customs officials say this one will be used at other border points in New Brunswick such as St. Stephen and Woodstock.
Source: http://nb.cbc.ca/regional/servlet/View?filename=nb_gammaport 20030911

12. *September 11, Globe and Mail* — **Scandinavian Airlines Systems to test biometrics.** Hoping to improve security while letting passengers through checkpoints more efficiently, Scandinavian Airlines Systems plans to test biometric technology at two airports. **Biometric systems examine people's fingerprints, irises or other characteristics to confirm their identities. Starting in November, SAS frequent flyers at Umeaa Airport in northern Sweden will have to let their fingerprints be scanned as they pass through a turnstile at the gate. A few weeks later, passengers at a yet−to−be determined airport in Scandinavia will have their irises scanned.** The tests will last six months and use SAS smart cards that have passengers' fingerprint and iris images already stored. Several airports worldwide have employed facial−recognition biometrics in hopes of nabbing wanted suspects, though the efficacy of the systems has been widely questioned. U.S. border crossings are due to get the technology next year.
Source: http://www.globetechnology.com/servlet/story/RTGAM.20030911.gtstocksep11/BNStory/Technology/

[Return to top]

## Postal and Shipping Sector

13. *September 11, DM News* — **USPS' NetPost. A private company has taken over management of the NetPost Mailing Online service formerly offered by the U.S. Postal Service (USPS). The company will own and operate NetPost under license to the USPS.** Launched in September 2000, NetPost was an experimental service that let small and midsized businesses send documents and mailing lists to the USPS, which then would send them to printers near their delivery point to maximize cost savings. The postal service announced the termination of the experiment earlier this month after three years. The company, which partnered with the USPS in 2000 to provide printing and mailing services as part of the original NetPost program, will take over the operation full−time in partnership with the Postal Service. The transition will be transparent to NetPost users.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2497 3

[Return to top]

## Agriculture Sector

14.

*September 11, Wisconsin Ag Connection* — **Crop drought damage. Wisconsin agricultural officials say the drought that has parched fields and dried up crops could cost farmers millions of dollars in crop losses.** The Farm Service Agency says that at the end of August, 56 percent of Wisconsin farm fields were very short of moisture and 27 percent were short. Meanwhile, Governor Jim Doyle declared a statewide drought emergency in mid−August. The dry weather will likely hit hardest the farmers without feed in reserve, said Don Hamm, president of the National Farmers Organization in Wisconsin. **The lack of rain will decrease crop yields, so farmers won't have as much feed. Most crops in Wisconsin are grown to feed cattle, hogs, and other farm animals.**
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=1089 &yr=2003

15. *September 11, USAgNet* — **Texas to start cattle TB testing.** Texas will soon begin working to regain its cattle tuberculosis (TB) free status. **Starting November 1, the state will implement the cattle TB plan developed by an industry and agency task force in 2002. The strategy includes testing dairy and purebred cattle herds. The surveillance testing, funded by the U.S. Department of Agriculture (USDA), is one element of the plan for regaining Texas' cattle TB−free status, which was granted in 2000, but revoked in 2002.** "To regain our TB−free status, we must prove to the USDA and to other states that we've conducted surveillance herd testing sufficient to identify and eliminate all cattle TB infection," says Bob Hillman, Executive Director of the Texas Animal Health Commission. "If testing reveals no additional infection, we could reapply for TB free status in August 2005. I believe we can regain our TB−free status," said Hillman. "The alternative is tantamount to throwing away nearly a century of disease eradication work. TB can damage our ability to market cattle freely, and if not addressed effectively, could destroy Texas' credibility as the country's leading cattle production state."
Source: http://www.usagnet.com/news−search.cfm?Id=973

16. *September 11, USAgNet* — **USDA survey shows breaches of biotech rules. The U.S. Department of Agriculture (USDA) found that almost 20 percent of the Midwestern farms growing a pest−resistant biotech crop have failed to comply with federal planting requirements.** The survey looked at 289,640 farms in 10 Midwestern states, Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Nebraska, Ohio, South Dakota and Wisconsin, to see how many were growing the biotech corn variety, Bt. It found that 93,530 farms, or 32 percent, were growing 4.2 million acres of Bt corn. **Of those, only about four−fifths were complying with an Environmental Protection Agency (EPA) requirement that farmers grow Bt corn in fields surrounded with conventional corn. This perimeter is meant to be a refuge to prevent pests from developing resistance to the Bt variety.** EPA spokesman Dave Deegan said the agency was still reviewing the survey. "We've not made any conclusions at this point," he said.
Source: http://www.usagnet.com/news−search.cfm?Id=975

17. *September 10, Guardian* — **Tropical virus may impact sheep. Bluetongue virus, spread by a tropical midge, has already crossed the Mediterranean and is being passed from one set of midge hosts to another in Britain, experts claim.** "It appears to have expanded its range northward and westward into areas where it has never been found before," Philip Mellor, of the Institute for Animal Health, told the British Association festival of science Wednesday. The virus carrier is a north African and Middle Eastern midge known as Cullicoides imicola, a

relative of the garden midge found in Britain. **The virus replicates in the cells lining the smaller blood vessels of animals. "It makes those blood vessels leaky and fragile, particularly in areas like the mouth, eyes and feet." The consequence is oedema. "You also get hemorrage," Mellor said.** "There will be an escape of blood into the mouth and conjunctivitis so secondary infections in and around the eyes. There will be damage to its hooves." He said the virus could also paralyse smooth muscle which could cause the sheep to suffer inhalation pneumonia. **The virus has been identified more than 500 miles north of its traditional range, and observers say a temperature rise of 2−5C could bring the infection to Britain.**
Source: http://www.guardian.co.uk/uk_news/story/0,3604,1038783,00.ht ml

[Return to top]

## Food Sector

18. *September 11, Iowa Ag Connection* — **U.S. beef company launching food safety treatment. The United States' fourth−largest beef packer, next month, will start spraying all of its products with a new food safety treatment aimed at protecting against food−borne illnesses. The treatment, derived from a milk−based protein known as lactoferrin, received final government approvals last month for use as a wash that detaches harmful bacteria from cattle carcasses.** It does not replace conventional methods aimed at sanitizing meat, such as irradiation, but adds another layer of protection for consumers, said the company's CEO John Miller. "We don't want to take any chances with food−borne illnesses," said Miller. "We liken this to a safety belt. It doesn't guarantee there won't ever be a problem, but it gives additional assurances." **The estimated cost of the new treatment is about $1 a head, which translates to about a half cent per pound.**
Source: http://www.iowaagconnection.com/story−state.cfm?Id=711&yr=20 03

[Return to top]

## Water Sector

19. *September 09, Environmental Protection Agency* — **EPA establishes new security division. G. Tracy Mehan III, Environmental Protection Agency's (EPA) Assistant Administrator for Water, announced Tuesday that the Agency has formed a new Water Security Division.** This Division will continue the work undertaken by the Water Protection Task Force established in October 2001. The original Task Force has awarded $51 million in grants directly to large drinking water systems to assist compliance with the requirements of the "Public Health Security and Bioterrorism Preparedness and Response Act of 2002." Out of 466 systems, 464 have submitted vulnerability assessments to EPA. **The Water protection Task Force has also awarded over $30 million in grants to the states, tribes, and non−profit organizations to provide tools, training, and technical assistance to small and medium drinking water systems as well as wastewater utilities on vulnerability assessments and related security work.** Additionally, the Task Force has supported the establishment of the WaterISAC, a state−of−the−art, secure information system that shares up−to−date threat and incident information between the intelligence community and the water sector. The new Water

Security Division will enhance these programs and accomplishments.
Source: http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/783e3921da458f6c85256d9c007a5c26?OpenDocument

[Return to top]

## Public Health Sector

20. *September 11, University of Wisconsin−Madison* — **Potent toxin reveals new antibiotic resistance mechanism. More and more, microbes are able to eliminate, modify, and sequester the toxic molecules that make up the antibiotics that humans use to treat infection, making drugs increasingly impotent. Scientists have discovered another way pathogens escape from drugs: self−sacrifice.** "It is a new paradigm for resistance," says Jon S. Thorson, a University of Wisconsin−Madison professor of pharmacy. "It points to the fact that bacteria continue to find new routes to evade these drugs." Soil bacteria use enediynes to create a buffer, which could overwhelm the slow−growing enediyne−producing bugs. But to survive in the toxic environment it creates, the microbe must have a way to survive its own poisons. To protect itself, the bacterium quickly deploys a protein that intercepts the misdirected enediyne before it finds and destroys the organism's DNA. "Instead of cleaving DNA, the enediyne cleaves the protein and thereby inactivates itself," says Thorson. These methods of evading their own chemical warfare agents tend to be shared among bacteria, says Thorson, and are at the root of antibiotic resistance among the pathogenic bacteria that also borrow the defense mechanisms.
Source: http://www.eurekalert.org/pub_releases/2003−09/uow−ptr090803 .php

21. *September 11, Associated Press* — **Researchers prolong shelf life of blood platelets. In a study, Harvard University researchers have demonstrated that adding a bit of sugar to isolated blood platelets can allow them to be refrigerated and usefully preserved for at least 12 days. That more than doubles the shelf life of the current technique used, which is to store the platelets at room temperature for only five days. Because of spoilage, more than 25 percent of all platelets taken from donated blood must be discarded.** Extending the shelf life of platelets would significantly improve the supply, experts said. Platelets play a central role in forming blood clots, an essential action to prevent uncontrolled bleeding in the body. Platelets are made in the bone marrow and typically live 10 to 12 days in the blood stream. That means the body has to constantly make more platelets to replace those that die. Many cancer and leukemia patients are unable to naturally replace their platelets. As a result, about 2 million patients a year require platelet transfusions to avoid possibly lethal, uncontrolled bleeding. **To get enough platelets for a single treatment, blood centers have to process four pints to six pints of donated blood.**
Source: http://www.thebostonchannel.com/health/2475720/detail.html

22. *September 10, Reuters* — **U.S.−Mexico at odds over West Nile spread. A Mexican resident has tested positive for what may be the country's first case of West Nile virus, according to a U.S. health expert, but Mexican officials question the result and want the test redone.** Texas health experts on Wednesday confirmed the disease in a resident of the Mexican border town of Ciudad Juarez, after the patient sought treatment in a hospital in neighboring El Paso, Texas. Officials are awaiting the results of tests on two other Ciudad Juarez residents, who were

also treated in Texas. "One of the cases is positively confirmed. There is no mistake. We may have the results of the other two later on Wednesday," said Efren Ornelas, epidemiology coordinator for the El Paso Health Department. **Oscar Velasquez, health director for Mexico's federal center for epidemiology, said his agency asked the U.S. Centers for Disease Control and Prevention to rerun the tests because results from Mexico's national laboratory show the patient testing negative for the virus. Mexican health officials do not accept that the human form of the disease has spread into Mexico, where it has so far only been confirmed in animals and birds.** One person died of West Nile virus in Mexico last year, but Mexican officials said he was infected in the United States.
Source: http://asia.reuters.com/newsArticle.jhtml?type=healthNews&st oryID=3423375

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

23. *September 11, Government Computer News* — **Simulations train firefighters with blaze but no burn. The National Institute of Standards and Technology (NIST) scientists are at work converting years−old fire modeling software, Fire Dynamic Simulator, and fire imaging software called Smokeview to display more quickly and realistically the smoke, hot air and other gases that erupt from fires and wind.** They envision a virtual reality setup, where firefighters would wear head gear that would display in 3−D the fire and smoke images originating from an SGI computer and playing out on two eight−foot screens. **While that scenario is still three to four years in development, Forney said, the NIST team hopes to give firefighters CDs loaded with intuitive, simulated role−playing software for computer training as early as next year.** Through the visualization upgrades, the software package will be able to render extremely complex, multistory fires, as well as scenarios of potential outcomes of a firefighter's decision, from opening a window to pointing a hose in a certain direction. Programs like this could minimize the training deaths of firefighters that occur each year.
Source: http://www.gcn.com/vol1_no1/daily−updates/23493−1.html

24. *September 11, Washington Post* — **First responders equipped for terror; training covers biological warfare. The worst fears of Maryland's Charles County emergency planners are revealed inside the cardboard boxes stacked in a drab government building in La Plata. One box contains an anthrax detection kit. Inside another is an instrument for gauging poisonous gases in the air. Folded neatly in other boxes are about 170 full−body suits, which, along with gas masks, will protect their wearers against biological and chemical agents.** And in the parking lot, there is a shiny new trailer, its side covered with words describing the crisis it is designed to meet: "Weapons of Mass Destruction." St. Mary's and Calvert counties have taken similar steps to respond to terrorist attacks. Southern Maryland emergency planners say the efforts illustrate the new duties thrust upon them in the two years

since the attacks of September 11, 2001. Since 2001, almost $2 million in federal and state grants have poured into the region to pay for new equipment for first responders. Charles, Calvert and St. Mary's each are forming, for the first time, hazardous material teams trained to respond to anything from an oil spill to chemical warfare. **Maryland homeland security officials say the counties also have taken an important step by coordinating their responses to a potential local terrorist attack.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A52842−2003Sep 10.html

25. *September 11, Global Security Newswire* — **Los Alamos researchers develop dirty bomb analysis technique.** Researchers at Los Alamos National Laboratory in New Mexico have developed a method for quickly identifying the components of a "dirty bomb" and discovering the culprits behind such an attack, the laboratory announced Wednesday. **Before this development, identifying the isotopes used in a radiological weapon was expected to take 24 hours or more, according to the laboratory. A team led by scientist Bennie Martinez has now developed a method to complete the work in as little as six hours.** "It's clear the method can identify a variety of radionuclides that might be present in dirty bomb debris," Martinez said. "Since the method is fairly simple and uses a minimum of equipment, we believe it could be forward deployed and could provide early data to law enforcement and others following a terrorist event."
Source: http://www.govexec.com/dailyfed/0903/091103gsn1.htm

[Return to top]

## Information and Telecommunications Sector

26. *September 12, CNET News.com* — **OracleWorld hit with bomb scare. Responding to a bomb threat, software maker Oracle ordered thousands of attendees at its OracleWorld conference in San Francisco, CA, to evacuate the Moscone convention center Wednesday**, September 10. The Moscone Center said it had received multiple threatening calls. **The San Francisco Police Department (SFPD) said they found no bombs after hours of searching. Oracle told the SFPD that as many as 11,000 people were at the conference**, according to one officer. No one had yet claimed responsibility for the threat, according to police. The Moscone Center, the SFPD and a Bay Area FBI office all received threatening calls about it, Sgt. Neville Gittens of SFPD said. An Oracle representative said the bomb threat was made against the Moscone Center, not Oracle.
Source: http://news.com.com/2100−1012−5074383.html?part=dht&tag=ntop

27. *September 11, General Accounting Office* — **GAO−03−1138T: Effective Patch Management is Critical to Mitigating Software Vulnerabilities. Attacks on computer systems−in government and the private sector−are increasing at an alarming rate, placing both federal and private−sector operations and assets at considerable risk**. By exploiting software vulnerabilities, hackers can cause significant damage. While patches, or software fixes, for these vulnerabilities are often well publicized and available, they are frequently not quickly or correctly applied. **The federal government recently awarded a contract for a governmentwide patch notification service designed to provide agencies with information to support effective patching. Fortyone agencies now subscribe to this service**. At the request of the Chairman of the Subcommittee on Technology, Information Policy,

Intergovernmental Relations, and the Census, GAO reviewed (1) two recent software vulnerabilities and related responses; (2) effective patch management practices, related federal efforts, and other available tools; and (3) additional steps that can be taken to better protect sensitive information systems from software vulnerabilities.
Source: http://www.gao.gov/new.items/d031138t.pdf

**Internet Alert Dashboard**

**Current Alert Levels**

| | |
|---|---|
| AlertCon: 2 out of 4<br>https://gtoc.iss.net | Security Focus ThreatCon: 2 out of 4<br>http://analyzer.securityfocus.com/ |

**Current Virus and Port Attacks**

| | |
|---|---|
| **Virus:** | #1 Virus in the United States: **WORM_LOVGATE.G**<br>Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| **Top 10 Target Ports** | 135 (epmap), 1433 (ms−sql−s), 137 (netbios−ns), 1434 (ms−sql−m), 445 (microsoft−ds), 80 (www), 139 (netbios−ssn), 21 (ftp), 4444 (CrackDown), 1026 (nterm)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

[Return to top]

# General Sector

**28.** *September 11, Reuters* — **North Korea halts work at nuclear facility. North Korea appears to have halted worked at its Yongbyon nuclear complex, center of its efforts to produce plutonium for atomic weapons, U.S. officials said on Thursday. But they stressed that the reason is not known.** They told Reuters possibilities include: Pyongyang has done this as political gesture to encourage negotiations with the United States; it has run into technical difficulties; or, more ominously, it has finished reprocessing fuel needed for half dozen or more nuclear bombs. "There's not much going on," one U.S. official said when asked about current activity at Yongbyon. Another U.S. official said: "I sense there may be a pause in the action but would be nervous about concluding that for certain."
Source: http://asia.reuters.com/newsArticle.jhtml?type=topNews&story ID=3428491

**29.** *September 10, U.S. Department of State* — **U.S. Department of State: Public Announcement concerning Worldwide Caution. With the second anniversary of the September 11, 2001, attacks upon us, the U.S. Government is seeing increasing indications that al Qaeda is preparing to strike U.S. interests abroad**. In the last few months, al Qaeda and its associated organizations have struck in the Middle East in Riyadh, in North Africa in Casablanca, and in East Asia in Indonesia. **It is therefore possible that European or Eurasian locations could**

**be venues for the next round of attacks**, possibly to closely coincide with the anniversary of the September 11 attack. It is expected that al Qaeda will strive for new attacks that will be more devastating than the September 11 attack, possibly involving nonconventional weapons such as chemical or biological agents. **There is also potential for al Qaeda to attempt a second catastrophic attack within the U.S**. Terrorist actions may include, but are not limited to, suicide operations, hijackings, bombings or kidnappings. These may also involve commercial aircraft and threats to include conventional weapons, such as explosive devices. **Terrorists do not distinguish between official and civilian targets**.
Source: http://travel.state.gov/wwc1.html

[Return to top]

## DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

### DHS/IAIP Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 |
| Subscription and Distribution Information | Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information. |

### Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

### DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.